UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/269,830	04/01/1999	ALFRED SCHEERHORN	2345/62	1687

26646 7590 12/15/2005

KENYON & KENYON
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
CALLAHAN, PAUL E	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 12/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 09/269,830	**Applicant(s)** SCHEERHORN ET AL.	
	Examiner Paul Callahan	**Art Unit** 2137	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 26 January 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☒ The Notice of Appeal was filed on *26 November 2005*. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☒ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *11-30*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

Matthew B. Smithers

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137

Continuation of 11. does NOT place the application in condition for allowance because: The applicant argues in traverse of the rejections of the claims found in the previous Office Action under 35 USC 102(b), by asserting that the prior art applied: Atalla 5,319,710, fails to identically teach the features of: "... authentication tokens used to authenticate both the signals and a transmission sequence of the signals; and that the authentication token to be compared with the transmitted authentication token received by the receiver is calculated before the transmission of the signals." Yet a carefull reading of Atalla shows that these features are indeed taught by the reference at the passages cited in the previous Office Action. .

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 11-13, 15, 16, 18, 19, 22, 23, 25, 27, and 29 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Atalla et al., US Patent 5,319,710 Jun. 7, 1994.

As per claim 11, 12, and 15, Atalla teaches a method for transmitting signals between a transmitter and a receiver, the method comprising: Calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase, (abstract), Calculating authentication tokens for the signals as a function of the data in a communication phase so as to authenticate both the signals and the transmission sequence of the signals, (abstract, fig. 1, col. 3 line 60 through col. 4 line 10). Atalla teaches generation of a random number (fig. 2A item 52). Atalla teaches a step wherein signals received by a receiver from a transmitter are accepted as authentic if the transmitted authentication token is found to match an authentication token calculated by the receiver (Abstract).Atalla teaches the authentication token calculation by the receiver is completed before actual transmission of the signals" (abstract, fig. 1, col. 3 line 60 through col. 4 line 10).

As per claim 13, Atalla teaches certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence (abstract, fig. 3A, 3B, col. 3 lines 60-68 and col. 4 lines 1-29), and wherein the authentication token of one of the signals transmitted at an i-th position is calculated as a function of the coding of the signal and coding of the respective position in the transmission sequence (col. 3 line 60 through col. 4 line 29).

As per claims 16 and 25, Atalla teaches certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence and wherein the authentication token of a one of the signals transmitted at an ith position is calculated as a function of the coding of all previously transmitted signals and the coding of the respective portion in the transmission sequence, (col. 2 line 49 through col. 3 line 25, col. 3 line 60 through col. 4 line 29).

As per claims 18, 19, and 27, Atalla teaches a cryptographic algorithm that includes a block cipher including DES (col. 4 lines 1-29).

As per claims 22, 23, and 29, Atalla teaches calculation of another token for authentication of the transmitter, the other token being subsequently transmitted so as to initialize the receiver for authentication of the transmitter and confirming the transmission sequences by non-intersecting m-bit strings (col. 5 lines 5-38).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 14, 17, 20, 21, 24, 26, 28, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atalla as applied to claim 11 above, and Official Notice taken as detailed below. Claims 24, 26, 28, and 30 are rejected under 35 USC 103(a) as being unpatentable over Atalla and Official Notice.

As per claims 14, 17 and 26, Atalla does not specifically teach the authentication token of the signal transmitted at the ith position is a bit-by-bit XORing of the of the coding of the one signal and the coding of the respective position in the transmission sequence. Atalla does teach such a combination producing the authentication token (col. 3 line 60 through col. 4 line 27) but not use of an XORing process. However the use of XOR functions in producing MAC codes is old and well known in the art or cryptographic authentication routines, therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated this feature into the system of Atalla. It would have been desirable due to the simplicity of implementation of the function and it's low computational overhead.

As per claims 20, 21 and 28, Atalla does not specifically teach production of a pseudo-random sequence via a block cipher

operating in a known output feedback mode. However Official Notice may be taken that generation of pseudorandom sequences in this manner are old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Atalla. It would have been desirable to do so as the block cipher is well quantified and the output true randomness can accurately be determined.

As per claims 24 and 30, Atalla teaches a method for transmitting signals between a transmitter and a receiver, the method comprising: Calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase, (abstract), Calculating authentication tokens for the signals as a function of the data in a communication phase so as to authenticate both the signals and the transmission sequence of the signals, (abstract, fig. 1, col. 3 line 60 through col. 4 line 10). Atalla teaches generation of a random number (fig. 2A item 52) certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence (abstract, fig. 3A, 3B, col. 3 lines 60-68 and col. 4 lines 1-29) and wherein the authentication token of one of the signals transmitted at an i-th position is calculated as a function of the coding of the signal and coding of the respective position in the transmission sequence (col. 3 line 60 through col. 4 line 29). Atalla teaches a step wherein signals received by a receiver from a transmitter are accepted as authentic if the transmitted authentication token is found to match an authentication token calculated by the receiver (Abstract).Atalla teaches the authentication token calculation by the receiver is completed before actual transmission of the signals" (abstract, fig. 1, col. 3 line 60 through col. 4 line 10). Atalla does not specifically teach the authentication token of the signal transmitted at the ith position is a bit-by-bit XORing of the coding of the one signal and the coding of the respective position in the transmission sequence. Atalla does teach such a combination producing the authentication token (col. 3 line 60 through col. 4 line 27) but not use of an XORing process. However the use of XOR functions in producing MAC codes is old and well known in the art or cryptographic authentication routines, therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated this feature into the system of Atalla. It would have been desirable due to the simplicity of implementation of the function and it's low computational overhead. Atalla teaches calculation of another token for authentication of the transmitter, the other token being subsequently transmitted so as to initialize the receiver for authentication of the transmitter and confirming the transmission sequences by non-intersecting m-bit strings (col. 5 lines 5-38).

Paul Ullah

12-9-05